Paper No. 39

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ERIC SPRUNK

Appeal No. 2000-1330
Application No. 08/972,835

HEARD: December 13, 2001

Before FLEMING, LALL, and BLANKENSHIP, ***Administrative Patent Judges.***

FLEMING, ***Administrative Patent Judge***.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the final rejection of claims 1 through 6, 8 through 20 and 23 through 31, all of the claims pending in the present application. Claims 7, 21 and 22 have been canceled.

The invention is directed to a method and apparatus for generating cryptographic keys with a concealed work factor. The system provides a high apparent work factor to maintain a

high level of security against attackers. At the same time, with knowledge of a secret distribution key, a government agency is presented with a lower work factor.

Independent claim 1 is reproduced as follows:

1. A method for providing a cryptographic key for cryptographically processing information, said method comprising the steps of:

(a) generating a first key according to a key generator scheme;

(b) reducing a key space of said first key in accordance with a key space reduction function; and

(c) distributing said reduced key space over a larger key space in accordance with a one-way key space distribution function to provide said cryptographic key; wherein:

said cryptographic key has an associated first work factor S for a person without knowledge of said key space distribution function; and

said cryptographic key has an associated second work factor W < S for a person with knowledge of said key space distribution function.

The Examiner relies on the following references:

Elander et al. (Elander) 5,323,464 June 21, 1994

Applied Cryptography, Bruce Schneier, CIP of 1993 and copyright of 1994.

Claims 1 through 6, 8 through 20 and 23 through 31 stand rejected under 35 U.S.C. § 103 as unpatentable over Elander.

Claims 26 through 31 stand rejected under 35 U.S.C. § 103 as being unpatentable over Elander in view of Schneier.

Rather than repeat the arguments of Appellant or Examiner, we make reference to the Briefs and Answer for the details thereon.[1]

OPINION

We will not sustain the rejection of claims 1 through 6, 8 through 20 and 23 through 31 under 35 U.S.C. § 103.

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of establishing a ***prima facie*** case of obviousness. **In re Oetiker**, 977 F.2d 1443, 1445, 24 USPQ 1443, 1444 (Fed. Cir. 1992). ***See also In re Piasecki***, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing that some objective teaching in the prior art or knowledge generally available to one of ordinary skill in the art suggests the claimed subject matter. ***In re Fine***, 837 F.2d 1071, 1074, 5

[1] Appellant filed an Appeal Brief on June 11, 1999. Appellant filed a Reply Brief on October 26, 1999. The Examiner mailed an Office communication on December 30, 1999 stating that the Reply Brief has been entered and considered.

USPQ2d 1596, 1598 (Fed. Cir. 1988). Only if this initial burden is met does the burden of coming forward with evidence or argument shift to the Appellants. ***Oetiker***, 977 F.2d at 1445, 24 USPQ at 1444. ***See also Piasecki***, 745 F.2d at 1472, 223 USPQ at 788 ("After a ***prima facie*** case of obviousness has been established, the burden of going forward shifts to the applicant.").

Appellant points out in the Brief and the Reply Brief that Appellant's independent claims 1 and 14 both require "distributing said reduced key space over a larger key space in accordance with a one-way key space distribution function." Appellant argues that this is not disclosed or suggested by the prior art. Appellant further argues that there is no motivation to modify Elander's teaching by replacing or augmenting the use of DEA encryption with a one way function to provide the encrypted weakened key (KWEAK) because KWEAK is not communicated over a weak channel. See page 3 of Appellant's Reply Brief.

We note that Appellant's claim 1 recites:

> distributing said reduced key space over a larger key space in accordance with a one-way key space

> distribution function to provide said cryptographic key; wherein: said cryptographic key has an associated first work factor S for a person without knowledge of said key space distribution function; and said cryptographic key has an associated second work factor W < S for a person with knowledge of said key space distribution function.

Also, we note that the only other independent claim, claim 14, is in the apparatus format which recites substantially the same limitations.

Upon our review of Elander, we fail to find that Elander teaches the above limitations. In column 9, line 39, through column 10, line 45, Elander discloses that Figure 3 is a block diagram illustration of two cryptographic systems, A and B, that communicates CDM keys via a strong key distribution channel 50 and communicate CDM-masked data via a weakened privacy channel 60. From the careful reading of Elander, we find that Elander's system provides a separate weak (CDM) and a strong (DEA) keys and does not teach a single apparently strong key that is weak for the government's use only. Although the Elander's final CDM key is weak, the CDM key K transmitted in Figure 3 is the strong key. We note that Appellant is claiming protecting the weak key with a one-way function, whereas Elander only protects the strong key with a

one-way function. Therefore, we fail to find that Elander teaches or suggest Appellant's claimed method recited in Appellant's claim 1 or a key distributor recited in Appellant's claim 14, lines 8 through 17. Furthermore, upon our review of Schneier, we fail to find that Schneier closes the gap.

The Federal Circuit states that "[t]he mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification." ***In re Fritch***, 972 F.2d 1260, 1266 n.14, 23 USPQ2d 1780, 1783-84 n.14 (Fed. Cir. 1992), ***citing In re Gordon***, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984). It is further established that "[s]uch a suggestion may come from the nature of the problem to be solved, leading inventors to look to references relating to possible solutions to that problem." ***Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc.,*** 75 F.3d 1568, 1573, 37 USPQ2d 1626, 1630 (Fed. Cir. 1996), ***citing In re Rinehart***, 531 F.2d 1048, 1054, 189 USPQ 143, 149 CCPA 1976) (considering the problem to be solved in a determination of

obviousness). The Federal Circuit reasons in ***Para-Ordnance Mfg. Inc. v. SGS Importers Int'l Inc.***, 73 F.3d 1085, 1088-89, 37 USPQ2d 1237, 1239-40 (Fed. Cir. 1995), that for the determination of obviousness, the court must answer whether one of ordinary skill in the art who sets out to solve the problem and who had before him in his workshop the prior art, would have been reasonably expected to use the solution that is claimed by the Appellants. However, "[o]bviousness may not be established using hindsight or in view of the teachings or suggestions of the invention." ***Para-Ordinance Mfg. v. SGS Importers Int'l***, 73 F.3d at 1087, 37***, USPQ2d at 1239, citing W.L. Gore & Assocs., Inc. v. Garlock, Inc.*** 721 F.2d at 1551, 1553, 220 USPQ at 311, 312-13. In addition, our reviewing court requires the PTO to make specific findings on a suggestion to combine prior art references. ***In re Dembiczak***, 175 F.3d 994, 1000-01,
50 USPQ2d 1614, 1617-19 (Fed. Cir. 1999).

In view of the foregoing, we have not sustained the rejection of claim 1 through 6, 8 through 20 and 23 through 31

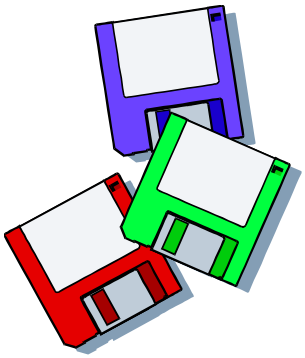
under 35 U.S.C. § 103. Accordingly, the Examiner's decision is reversed.

REVERSED

MICHAEL R. FLEMING Administrative Patent Judge	)
PARSHOTAM S. LALL Administrative Patent Judge	) BOARD OF PATENT APPEALS AND INTERFERENCES
HOWARD B. BLANKENSHIP Administrative Patent Judge	)

MRF/LBG

BARRY R. LIPSITZ
BRADFORD GREEN
755 MAIN STREET
MONROE, CT 06468



Lesley

Appeal No. 2000-1330
Application No. 08/972,835

APJ FLEMING

APJ BLANKENSHIP

APJ LALL

DECISION: REVERSED

Prepared: August 21, 2002

Draft Final

3 MEM. CONF. Y N

OB/HD GAU 2100

PALM / ACTS 2 / BOOK

DISK (FOIA) / REPORT